JC20 Rec'd PCT/PTO 26 JUL 20

FORM PTO-1390 (REV. 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY 'S DOCKET NUMBER
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		018926-003900US
		U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/890180
INTERNATIONAL APPLICATION NO. PCT/US00/02174	INTERNATIONAL FILING DATE January 28, 2000	PRIORITY DATE CLAIMED January 29, 1999

TITLE OF INVENTION: KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT SIGNALING AND CALL PACKETS BETWEEN CTA'S

APPLICANT(S) FOR DO/EO/US: SASHA MEDVINSKY; STEVEN E. ANDERSON; PAUL MORONEY; ERIC SPRUNK; JONATHAN A. FELLOWS

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST submission of items concerning a filing under 35 U.S.C. 371.**
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 36 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 37(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau
   c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)).
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.2 and 35 U.S.C. 1.821 – 1.825.
18. ☐ A second copy of the published international application under 36 U.S.C.
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:

5 sheets formal drawings

JC18 Rec'd PCT/PTO 26 JUL 2001

I/S/ Application no. (if known, see 37 CFR 1.5) 09/890180	INTERNATIONAL APPLICATION NO. PCT/US00/02174	ATTORNEY'S DOCKET NUMBER 018926-003900US

21. ☒ The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492(A) (1) – (5)):		
Neither international preliminary examination fee (37 CFR 1.492) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search report prepared by the EPO of JPO **$860.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)(4).....**$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	**$690**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	10 - 20 =		x **$18.00**	$	
Independent claims	3 -3 =		x **$80.00**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **270.00**	$	
TOTAL OF ABOVE CALCULATIONS =				**$690**	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +				$	
SUBTOTAL =				**$690**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFT 1.492(f).				$	
TOTAL NATIONAL FEE =					
Fee for recording the enclosed assignment (37 CFR 1.2(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
TOTAL FEES ENCLOSED =				**$690**	
				Amount to be refunded:	$
				charged:	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 20-1430 in the amount of $690 to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 20-1430. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Charles J. Kulas
Townsend and Townsend and Crew LLP
Two Embarcadero Center, 8th fl.
San Francisco, CA 94111

SIGNATURE

Charles J. Kulas
NAME

35,809
REGISTRATION NUMBER

KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT SIGNALING AND CALL PACKETS BETWEEN CTA'S

CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims priority from a U.S. Provisional Patent Application 60/117,788 filed on January 29, 1999 and from a U.S. Provisional Patent Application 60/128,772 filed on April 9, 1999, the disclosures of which are incorporated in their entirety herein by reference for all purposes.

FIELD OF THE INVENTION

This invention relates to the field of communication in telephony networks, and more particularly, to the establishment of a secure communication channel between users in an IP telephony network.

BACKGROUND OF THE INVENTION

Internet Protocol (IP) telephony networks allow large numbers of users to communicate with each other over secure channels. Typically, a user is coupled to the IP telephony network via a telephony adapter (TA). In a cable IP networks, a cable telephony adapter (CTA) may be used. The CTA converts user information, such as voice or data, into packets for transmission on the network, and converts received packets into digital or analog signals for use by the user.

To implement a secure channel between two users in the IP telephony network, their associated CTAs use the same encryption techniques and keys. However, this presents a problem since for CTA to CTA communications, there is a very large number (millions) of possible connections that may be established. Thus, any single CTA cannot possibly maintain security associations for all possible connections ahead of time. Therefore a security association (e.g. encryption key) must be established on the fly--when the secure channel (phone call) is first set up.

Standard techniques to establish CTA to CTA communications provide secure key exchanges (authenticated and confidential), and use one of two techniques. In the first technique, a known key is shared between the two parties. As stated above, this technique does not scale to millions of users and is therefore not applicable for general IP telephony networks. The second technique, uses a public key technique, such as Diffie-Hellman exchanges in combination with digital signatures. Such techniques are costly in terms of time and CPU consumption and may cause a noticeable delay in call setup or increase the cost of the CTA device. Thus, public key techniques are not desirable for this purpose.

SUMMARY OF THE INVENTION

The present invention provides a system for establishing secure communication between users in an IP telephony network. In IP telephony networks, gateway controllers are used to control messaging between the users and the IP telephony network infrastructure.

The system included in the present invention provides a gateway controller that creates a media stream encryption key that is used to encrypt and decrypt messages between users. When a first user attempts to establish a secure channel with a second user, the gateway controller (source) associated with the first user, creates the media stream encryption key, sends the key inside a signaling message to the gateway controller (destination) that services the second user. The two gateway controllers then send the key to the two CTAs, that service the first and second users. This allows the two CTAs, and thus, the two users to quickly establish a secure communication channel in the IP telephony network.

In an embodiment of the present invention a method for establishing a secure communication channel between a first user and a second user in an IP telephony network is provided. The first user and the second user are coupled to first and second telephony adapters, which in turn, are coupled to first and second gateway controllers, respectively, wherein the gateway controllers control user access to the IP telephony network. The telephony adapters are used to encrypt and decrypt user information exchanged over the IP telephony network. The method begins by receiving a request at the first gateway controller to establish a secure communication channel between the first user and the second user. Next, a secret key is generated at the first gateway controller.

A copy of the secret key is distributed to the first and second telephony adapters over previously established secure connections. Finally, the secure communication channel is established between the first user and the second user by encrypting and decrypting information using the secret key.

A further understanding of the nature and the advantages of the inventions disclosed herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a portion of an IP telephony network constructed in accordance with the present invention;

FIG. 2 shows a gateway controller constructed in accordance with the present invention.

FIG. 3 shows a message flow diagram illustrating message flow in the IP telephony network of FIG. 1 in accordance with the present invention;

FIG. 4 shows a method for establishing a secure communication channel between users in the IP telephony network of FIG. 1 using the messages shown in FIG. 3; and

FIG. 5 shows the IP telephony network of FIG. 1 and includes a connection to a plain old telephone system (POTS) gateway.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

The present invention includes a system for establishing a secure communication channel between users of an IP telephony network. Embodiments of the present invention utilize key-based encryption techniques as a mechanism for achieving secure communication in the IP telephony network. Such embodiments are not limited to using any one encryption technique, and therefore, it is possible to construct embodiments of the present invention using several types of encryption techniques. Since the type of encryption technique selected is not essential to the embodiments of the present invention, a detailed description of a specific encryption technique is not provided.

For purposes of clarity and convenience, it will be assumed that the IP telephony network is a cable network, and so, cable telephony adapters (CTA) will be used in the various embodiments. However, the invention is not limited to using CTAs,

and may in fact be implemented using any other type of telephony adapters as required by a particular network.

FIG. 1 shows a portion of an IP telephony network 100 constructed in accordance with the present invention. The network 100 includes a first user 102 coupled to a source CTA 104. The source CTA 104 is further coupled to a source gateway controller 106 and an IP telephony network backbone 110.

The network 100 also includes a second user 112 coupled to a destination CTA 114. The destination CTA 114 is further coupled to a destination gateway controller 116 and the IP telephony network backbone 110. In addition, the network 100 also includes a customer service representative (CSR) center 120, a provisioning server 122 and a billing host 124.

Each user of the network 100 goes through an initialization process to activate network service. For example, when the user 102 and associated CTA 104 are coupled to the network, a series of messages are exchanged between the CTA 104, the gateway controller 106 and the CSR 120. The messages provide for activation of telephony service for the user 102, establishment of account information and creation of encryption keys to be used by the CTA to encrypt and decrypt messages exchanged over the network. The billing host 124 is used to setup account information for each user and to bill for network usage. The provisioning server 122 is used to initialize and register CTA devices within a specific IP telephony network.

FIG. 2 shows one embodiment of a gateway controller 200 constructed in accordance with the present invention. The gateway controller 200 includes a message processor 202, a key creation module 204 and a key storage 206. The gateway controller 200 is coupled between the IP telephony backbone and a network adapter, such as a CTA device. For example, the gateway controller 200 is suitable for use as the gateway controller 106 in FIG. 1.

The message processor 202 processes messages that are exchanged between the CTA and other components of the telephony network. For example, when messages are exchanged between the CTA and other components of the network during an initial CTA registration process.

The key creation module 204, has logic to create or derive keys that may be used to encrypt or decrypt messages exchanged between CTAs over the IP telephony backbone 110. The keys may be stored in the key storage 206. The key storage has logic

to encrypt the keys before storage using a public/private key pair. For example, the public/private key pair may be provided by the network 100 infrastructure or from government law enforcement officials.

FIG. 3 shows a message exchange diagram 300 illustrating how messages are exchanged between the components of the network 100 to establish a secure communication channel between the user 102 and the user 112. The messages are transmitted or received at the source CTA represented at line 302, the source gateway controller 106 represented at line 304, the destination gateway controller 116 represented at line 306, and the destination CTA 114 represented at line 308.

FIG. 4 shows a flow diagram 400 illustrating the process of establishing a secure communication channel utilizing the messages shown in FIG. 3 in accordance with the present invention.

At block 402, secure call signaling between the source and destination gateway controllers is established as shown by message 310. At block 404, secure call signaling between source and destination CTAs and their associated gateway controller is established as shown by messages 312 and 314.

At block 406, the user 102 desires to place a secure call to the user 112 and so notifies the CTA 104 which in turn notifies the gateway controller 106, as shown by message 316 and at path 130. At block 408, the source gateway controller creates a key to be used to establish the secure communication channel requested by the user 102. In one embodiment, the key is a random number and may be generated, for example, at the key creation module 204.

At block 410, the key is transmitted from the source gateway controller to the destination gateway controller, as shown by message 318 and at path 132. At block 412, the destination gateway controller forwards the key to the destination CTA as shown by message 320 and at path 134. At block 414, the destination CTA sends an acknowledgment to the destination gateway controller indicating that the key has been received, as shown by message 322 at path 136.

At block 416, the destination gateway controller sends an acknowledgment to the source gateway controller indicating that the key has been received, as shown by message 324 at path 138. At block 418, the source gateway controller transmits the key to the source CTA, as shown by message 326 at path 140. At block 420, the source CTA responds by transmitting an acknowledgment as shown by message 328 at path 142.

At block 422, a secure channel between the source CTA and the destination CTA can now be established where encrypted messages can be exchanged between the telephony users 102 and 112, as shown by message 330 at path 144.

As a result of the above described operations, the source gateway controller creates an encryption key and distributes it to the source and destination CTAs to quickly set up a secure communication channel thereby allowing the user 102 and the user 112 to communicate over the IP telephony network 100. In one embodiment the messages distributing the key are additional messages used to operate the network 100. In another embodiment, the key may be incorporated into existing call signaling messages so as to keep of the overall message overhead low and improve network efficiency.

FIG. 5 shows the IP telephony network 100 of FIG. 1 and includes a connection to a plain old telephone system (POTS) gateway 504. The POTS gateway 504 is coupled to a third user 502 of the network 100.

To establish a secure communication channel between the user 102 and the user 502, the method of FIG. 4 can be used, however, since there is no destination CTA, operations relating to the destination CTA are not used. For example, the POTS gateway can provide a private and authenticated connection. Thus, the following describes the differences in the call setup process when using the POTS gateway.

At block 410, the source gateway controller sends the key to the POTS gateway 504, as shown by path 506. The blocks 412 and 414 are skipped. At block 416, the POTS gateway sends an acknowledge signal to the source gateway controller as shown by path 508. Blocks 418 through 422 remain the same.

Using the above modifications to the method of FIG. 4, a private and authenticated secure channel can be established between the CTA 104 and the POTS gateway 504, as shown at path 520, so that the users 102 and 504 may exchange messages.

In another embodiment of the present invention, where the call origination is reversed, the encryption key can be requested from the destination gateway. For example, the user 502 requests to make a call to user 102. The POTS gateway 504 requests the encryption key from the gateway controller 106, which services the user 102. The gateway controller 106 then creates the encryption key and provides it to the POTS gateway to allow a secure communication channel to be created between the POTS gateway and the CTA 104.

In another embodiment of the present invention, the encryption key can be created at the source gateway controller by deriving it from a secret already shared between the source gateway controller and the source CTA. Thus, both the source gateway controller and the source CTA can derived the key from the shared secret. In this embodiment, it is not necessary for the source gateway controller to transmit the key to the source CTA after it has been distributed to the destination CTA. This results in fewer messages being exchanged to setup the secure channel between the users.

In another embodiment of the present invention, the key created at the source gateway controller can be shared with law enforcement. The Communications Assistance for Law Enforcement Act (CALEA) requires that phone systems allow the government access to conversations flowing within their networks for wire-tapping purposes. To facilitate this, a CALEA server 510 may be included in the network 100 as shown in FIG. 5. The CALEA server can be accessed by law enforcement, either directly, as shown by 512, or from some other location within the network 100.

The source gateway controller may operate in several ways to comply with the CALEA requirements. In a first method of operation, the source gateway controller receives a request 514 from the CALEA server to forward any key created for use with a particular user. For example, when the user 102 requests to make a call and a key is created, the key is transmitted to the CALEA server, as shown at 516. In a second method of operation, the source gateway controller receives a request 514 to forward any key currently being used by a particular user. For example, if the user 102 already has a call established using a particular key, that key is transmitted to the CALEA server, as shown at 516. In a third method of operation, the source gateway controller receives a request 514 to forward any key previously used by a particular user. For example, if the user 102 had previously made a call using a particular key, that key is stored in the key storage 206 of the gateway controller. The key is retrieved from the key storage and transmitted to the CALEA server as shown at 516.

In one embodiment, the keys are encrypted prior to storage. The encryption is done using a public/private key pair belonging to law enforcement. Thus, upon retrieval, any keys so encrypted can only be decrypted by law enforcement officials with knowledge of the private key.

Once the key is at the CALEA server, messages are redirected by the network to the server so that they may be decoded using the key and monitored by law

enforcement officials. Thus, embodiments of the gateway controller of the present invention includes support for the CALEA requirements.

The present invention provides a method and apparatus for establishing a secure communication channel between two users in a telephony network. It will be apparent to those with skill in the art that modifications to the above methods and embodiments can occur without deviating from the scope of the present invention. Accordingly, the disclosures and descriptions herein are intended to be illustrative, but not limiting, of the scope of the invention which is set forth in the following claims.

WHAT IS CLAIMED IS:

1. A method for establishing a secure communication channel in an IP telephony network between a first and a second user, wherein the first user and the second user are coupled to first and second telephony adapters, which in turn, are coupled to first and second gateway controllers, respectively, wherein the gateway controllers control user access to the IP telephony network, and wherein the telephony adapters encrypt and decrypt user information exchanged over the IP telephony network, the method comprising:

receiving a request at the first gateway controller to establish a secure communication channel between the first user and the second user;

generating a secret key at the first gateway controller;

distributing the secret key to the first and second telephony adapters over previously established secure connections; and

establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key.

2. The method of claim 1 wherein the step of generating comprises a step of generating a random number at the first gateway controller to be used as the secret key.

3. The method of claim 1 wherein the step of generating comprises a step of deriving the secret key at the first gateway controller, wherein the secret key is derived from a signaling key shared between the first telephony adapter and the first gateway controller.

4. The method of claim 1 wherein the step of distributing comprises steps of:

transmitting the secret key from the first gateway controller to the second gateway controller;

transmitting the secret key from the second gateway controller to the second telephony adapter

transmitting the secret key from the first gateway controller to the first telephony adapter.

5. The method of claim 1 further comprising steps of;

receiving a request at the first gateway controller to provide the secret key to a law enforcement server; and

providing the secret key to the law enforcement server.

6. An IP telephony network for establishing a secure communication channel between a first user and a second user, wherein the first user and the second user are coupled to first and second telephony adapters, which in turn, are coupled to first and second gateway controllers, respectively, wherein the gateway controllers control user access to an IP telephony backbone, and wherein the telephony adapters encrypt and decrypt user information exchanged over the IP telephony network, the IP telephony network comprising:

means for receiving a request at the first gateway controller to establish a secure communication channel between the first user and the second user;

means for generating a secret key at the first gateway controller;

means for distributing the secret key to the first and second telephony adapters over a previously established secure connection; and

means for establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key.

7. A gateway controller for establishing a secure communication channel in an IP telephony network, the gateway controller coupled between a telephony adapter and a telephony network backbone, the gateway controller comprising:

a key creation module having logic to create a secret key;

a key storage module coupled to the key creation module and having logic to store the secret key; and

a message processor coupled to the key creation module and the key storage module, and having logic to process messages exchanged between the telephony adapter and the telephony network backbone, wherein the message processor further comprises:

logic to receive a request to establish a secure communication channel between a first user and a second user, the first user couple to the telephony adapter, the second user coupled to a remote telephony adapter;

logic to distributed the secret key to the telephony adapters over previously established secure connections, whereby the secure communication channel between the first user and the second user may be established by encrypting and decrypting information using the secret key.

8. The gateway controller of claim 7 wherein the key creation module has logic to generate a random number as the secret key.

9. The gateway controller of claim 7 wherein the key creation module has logic to derive the secret key from a signaling key shared with the telephony adapter.

10. The gateway controller of claim 7 wherein the key storage module has logic to encrypt the secret key before storage, using a public/private key pair belonging to law enforcement.

SUBSTITUTE SHEET (RULE 26)

20m210 D0T0656D

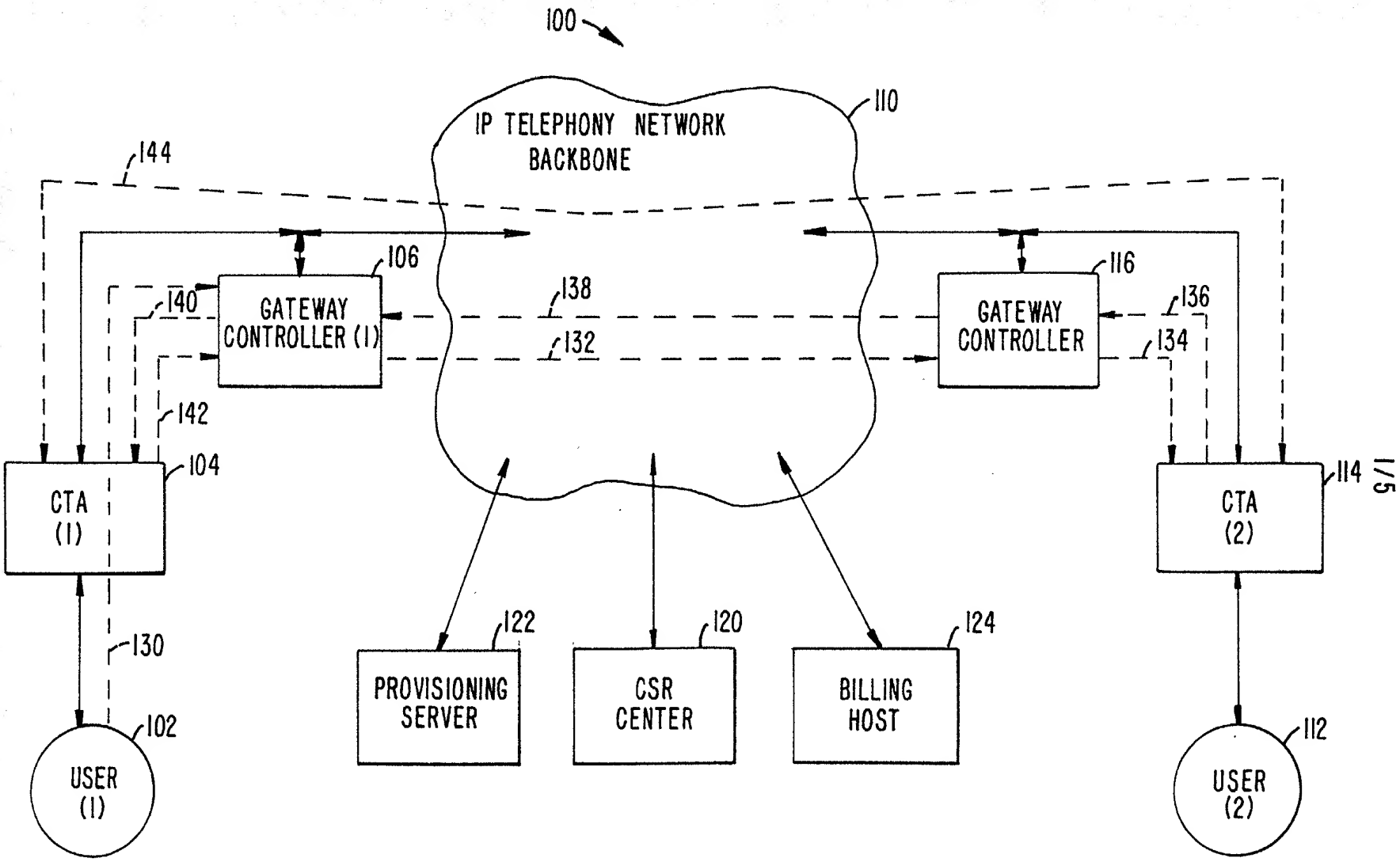

FIG. 1.

09/890180

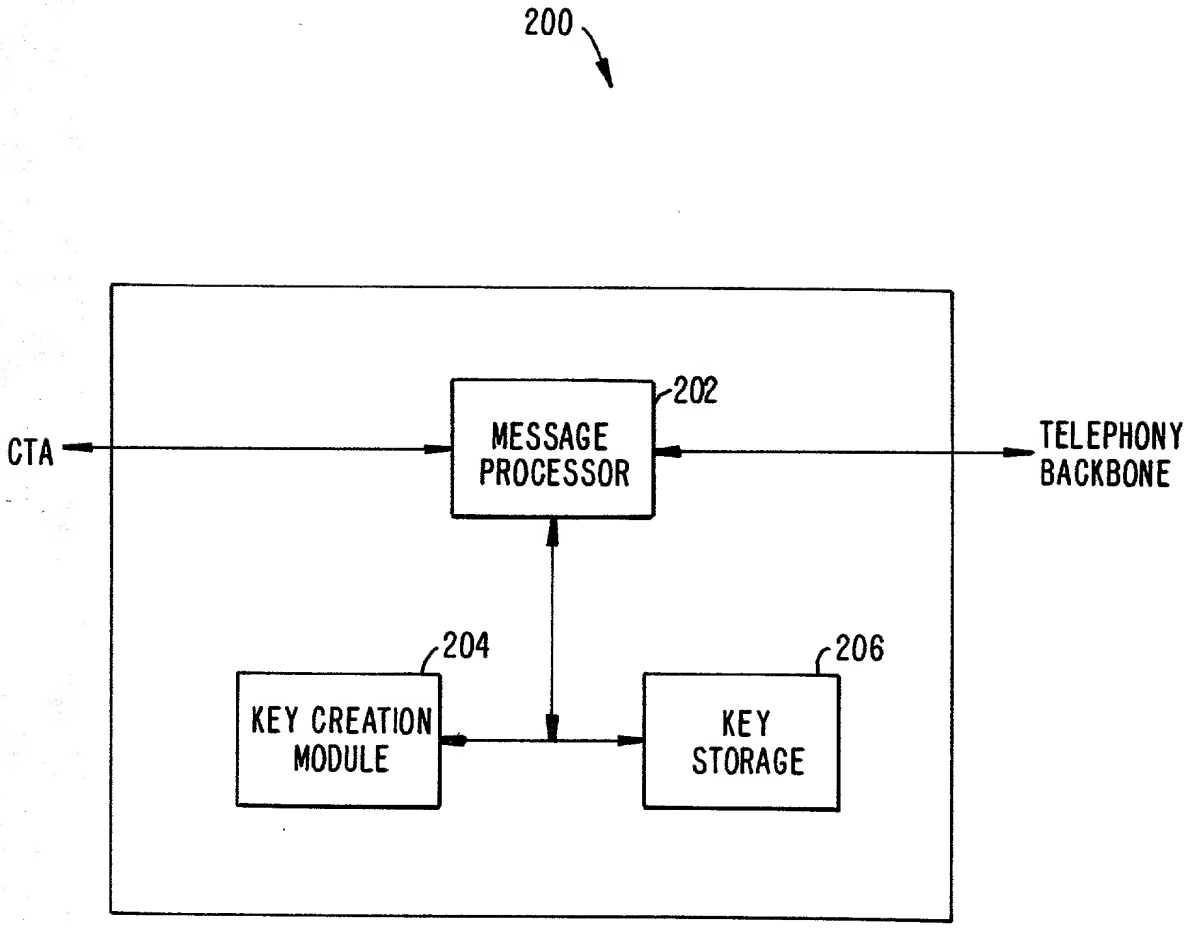
200
CTA
MESSAGE PROCESSOR
202
TELEPHONY BACKBONE
204
KEY CREATION MODULE
206
KEY STORAGE

FIG. 2.

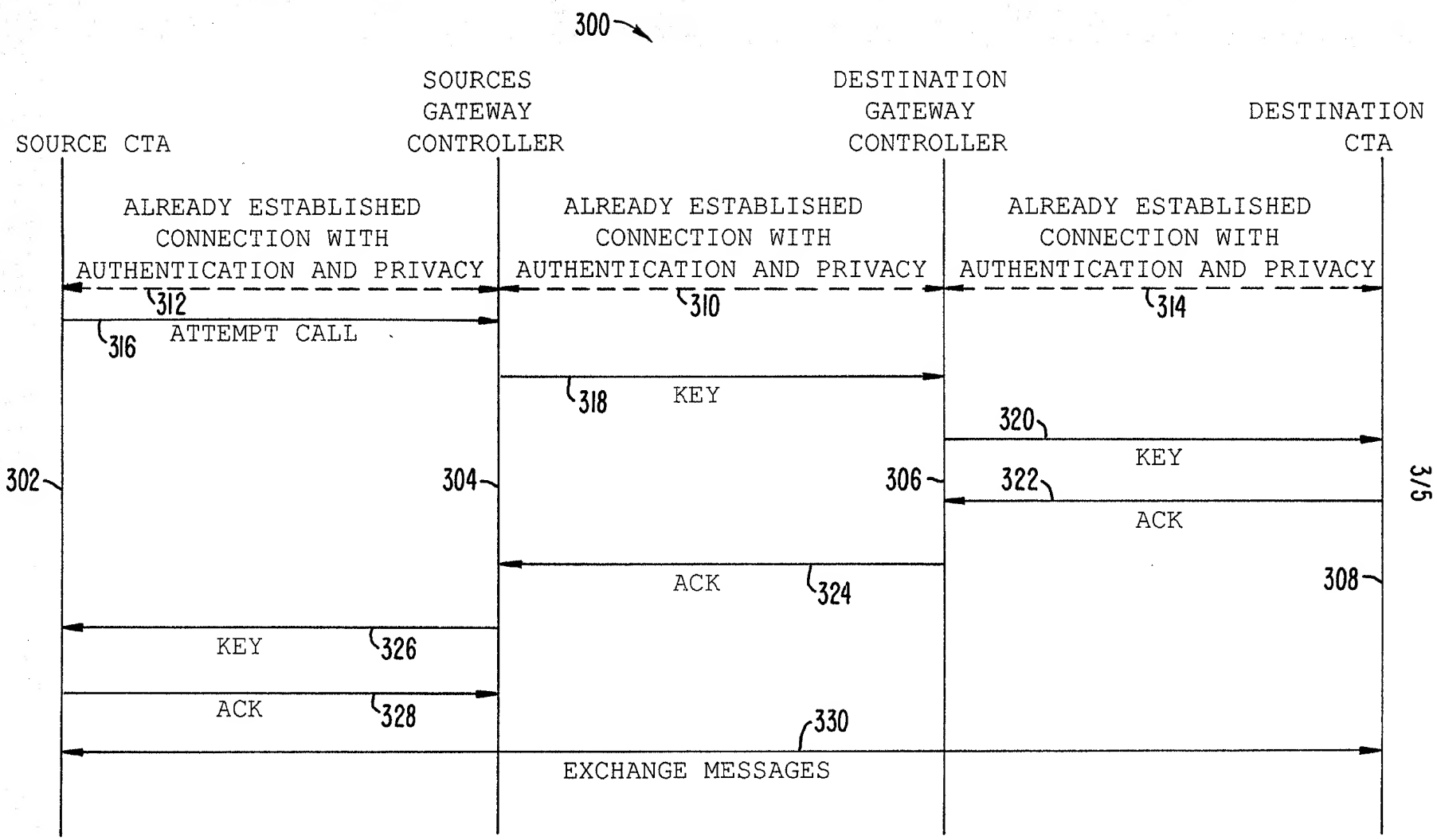

FIG. 3.

09/890180

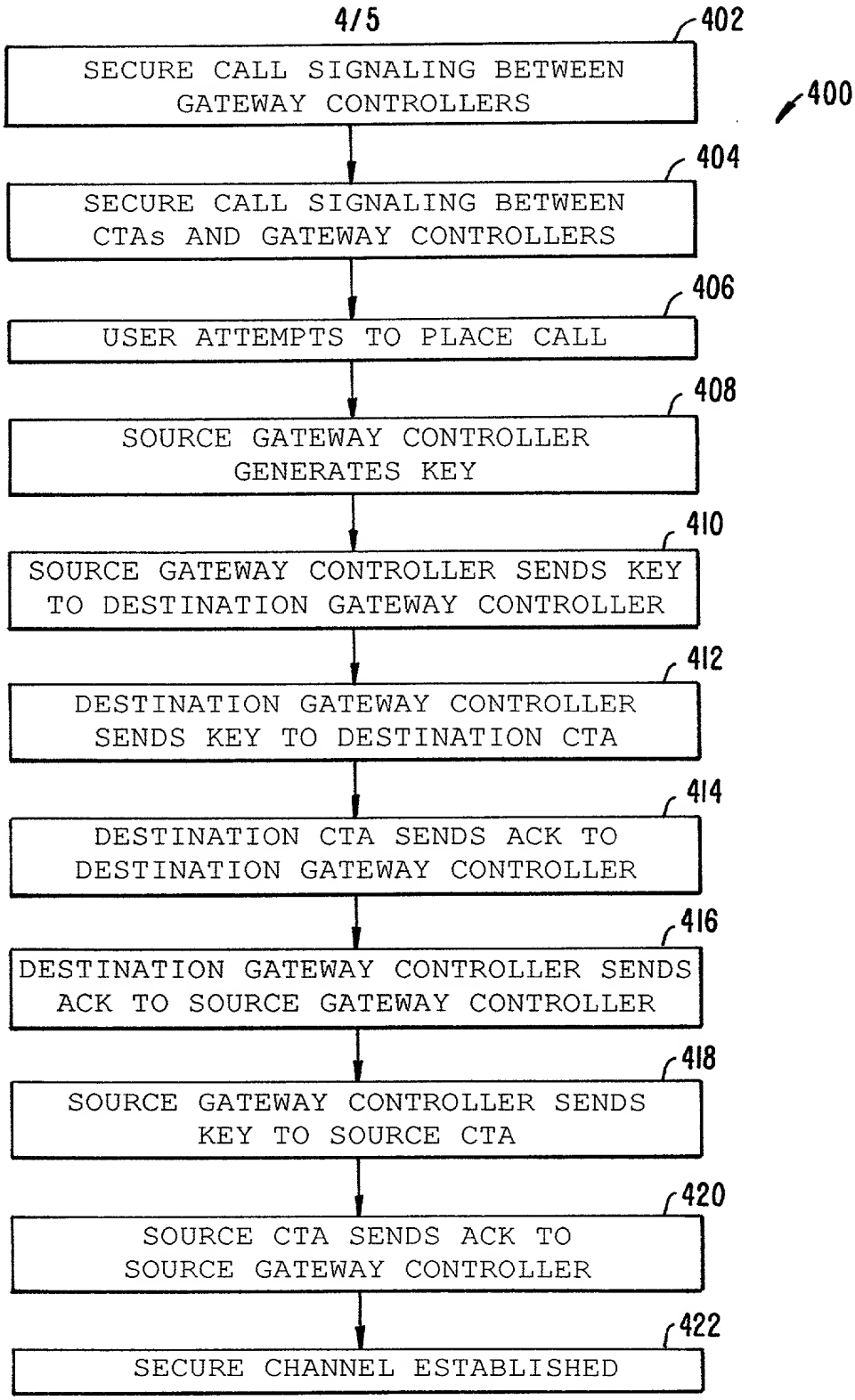
SECURE CALL SIGNALING BETWEEN GATEWAY CONTROLLERS
402
400
SECURE CALL SIGNALING BETWEEN CTAs AND GATEWAY CONTROLLERS
404
USER ATTEMPTS TO PLACE CALL
406
SOURCE GATEWAY CONTROLLER GENERATES KEY
408
SOURCE GATEWAY CONTROLLER SENDS KEY TO DESTINATION GATEWAY CONTROLLER
410
DESTINATION GATEWAY CONTROLLER SENDS KEY TO DESTINATION CTA
412
DESTINATION CTA SENDS ACK TO DESTINATION GATEWAY CONTROLLER
414
DESTINATION GATEWAY CONTROLLER SENDS ACK TO SOURCE GATEWAY CONTROLLER
416
SOURCE GATEWAY CONTROLLER SENDS KEY TO SOURCE CTA
418
SOURCE CTA SENDS ACK TO SOURCE GATEWAY CONTROLLER
420
SECURE CHANNEL ESTABLISHED
422

FIG. 4.

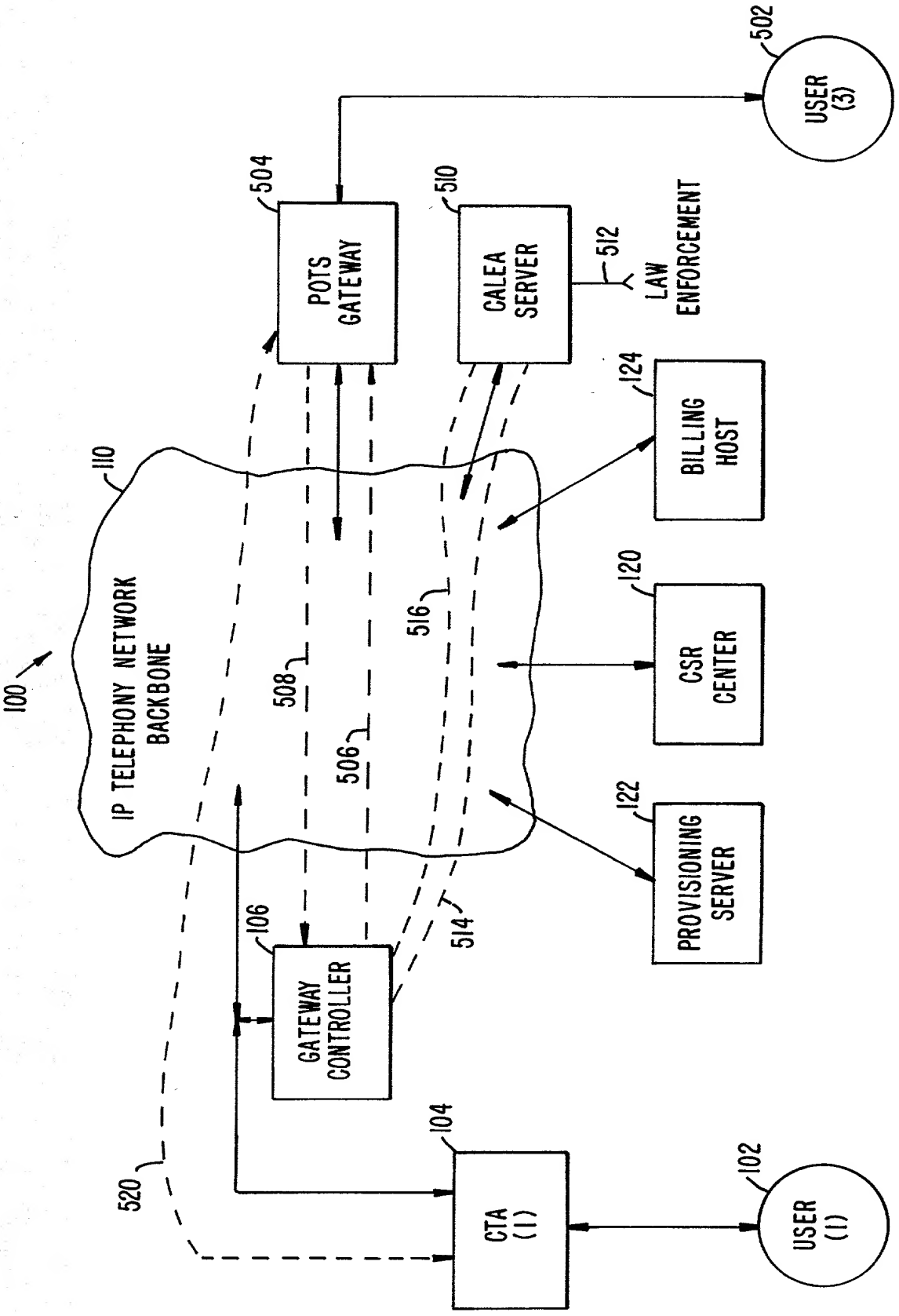
100
110
IP TELEPHONY NETWORK BACKBONE
502
USER (3)
504
POTS GATEWAY
510
CALEA SERVER
512
LAW ENFORCEMENT
124
BILLING HOST
120
CSR CENTER
122
PROVISIONING SERVER
106
GATEWAY CONTROLLER
104
CTA (1)
102
USER (1)
508
506
516
514
520

FIG. 5.

Rec'd PCT/PTO 24 JUL 2001

Attorney Docket No.: 018926-003900US
Client Reference No.: D2429

09/890180

DECLARATION

As a below named inventor, I declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT SIGNALING AND CALL PACKETS BETWEEN CTA'S** the specification of which ____ is attached hereto or _X_ **was filed as U.S. Application No. 09/890,180 the National Phase of PCT/US00/02174, filed January 28, 2000** and was amended on _____ (if applicable). and was amended on _____ (if applicable).

I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56. I claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Country	Application No.	Date of Filing	Priority Claimed Under 35 USC 119

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

Application No.	Filing Date
60/117,788	January 29, 1999
60/128,772	April 9, 1999

I claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application No.	Date of Filing	Status

Full Name of Inventor 1:	Last Name: **MEDVINSKY**	First Name: **ALEXANDER**	Middle Name or Initial:	
Residence & Citizenship:	City: **San Diego**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **8873 Hampe Court**	City: **San Diego**	State/Country: **California**	Postal Code: **92129**

Full Name of Inventor 2:	Last Name: **ANDERSON**	First Name: **STEVEN**	Middle Name or Initial: **E.**	
Residence & Citizenship:	City: **San Diego**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **5521 Taft Avenue**	City: **San Diego**	State/Country: **California**	Postal Code: **92037**
Full Name of Inventor 3:	Last Name: **MORONEY**	First Name: **PAUL**	Middle Name or Initial:	
Residence & Citizenship:	City: **Olivenhain**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **3411 Western Springs Road**	City: **Olivenhain**	State/Country: **California**	Postal Code: **92024**
Full Name of Inventor 4:	Last Name: **SPRUNK**	First Name: **ERIC**	Middle Name or Initial: **J.**	
Residence & Citizenship:	City: **Carlsbad**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **7309 Bolero Street**	City: **Carlsbad**	State/Country: **California**	Postal Code: **92009**
Full Name of Inventor 5:	Last Name: **FELLOWS**	First Name: **JONATHAN**	Middle Name or Initial: **A.**	
Residence & Citizenship:	City: **Del Mar**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **13161 Shalimar Pl.**	City: **Del Mar**	State/Country: **California**	Postal Code: **92014**

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature of Inventor 1	Signature of Inventor 2	Signature of Inventor 3
Alexander Medvinsky	Steven E. Anderson	Paul Moroney
Date 11-26-2001	Date	Date 11-26-2001
Signature of Inventor 4	**Signature of Inventor 5**	
Eric J. Sprunk	Jonathan A. Fellows	
Date 11-29-01	Date	

Full Name of Inventor 2:	Last Name: **ANDERSON**	First Name: **STEVEN**	Middle Name or Initial: **E.**	
Residence & Citizenship:	City: **San Diego**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **5521 Taft Avenue**	City: **San Diego**	State/Country: **California**	Postal Code: **92037**
Full Name of Inventor 3:	Last Name: **MORONEY**	First Name: **PAUL**	Middle Name or Initial:	
Residence & Citizenship:	City: **Olivenhain**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **3411 Western Springs Road**	City: **Olivenhain**	State/Country: **California**	Postal Code: **92024**
Full Name of Inventor 4:	Last Name: **SPRUNK**	First Name: **ERIC**	Middle Name or Initial: **J.**	
Residence & Citizenship:	City: **Carlsbad**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **7309 Bolero Street**	City: **Carlsbad**	State/Country: **California**	Postal Code: **92009**
Full Name of Inventor 5:	Last Name: **FELLOWS**	First Name: **JONATHAN**	Middle Name or Initial: **A.**	
Residence & Citizenship:	City: **Del Mar**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **13161 Shalimar Pl.**	City: **Del Mar**	State/Country: **California**	Postal Code: **92014**

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature of Inventor 1 Alexander Medvinsky Date 11-26-2001	Signature of Inventor 2 Steven E. Anderson Date 12/7/2001	Signature of Inventor 3 Paul Moroney Date 11-26-2001
Signature of Inventor 4 Eric J. Sprunk Date 11-29-01	Signature of Inventor 5 Jonathan A. Fellows Date	

Full Name of Inventor 2:	Last Name: **ANDERSON**	First Name: **STEVEN**	Middle Name or Initial: **E.**	
Residence & Citizenship:	City: **San Diego**	State/Foreign Country: **California**	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **5521 Taft Avenue**	City: **San Diego**	State/Country: **California**	Postal Code: **92037**
Full Name of Inventor 3:	Last Name: **MORONEY**	First Name: **PAUL**	Middle Name or Initial:	
Residence & Citizenship:	City: **Olivenhain**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **3411 Western Springs Road**	City: **Olivenhain**	State/Country: **California**	Postal Code: **92024**
Full Name of Inventor 4:	Last Name: **SPRUNK**	First Name: **ERIC**	Middle Name or Initial: **J.**	
Residence & Citizenship:	City: **Carlsbad**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **7309 Bolero Street**	City: **Carlsbad**	State/Country: **California**	Postal Code: **92009**
Full Name of Inventor 5:	Last Name: **FELLOWS**	First Name: **JONATHAN**	Middle Name or Initial: **A.**	
Residence & Citizenship:	City: **Del Mar**	State/Foreign Country: **California** CA	Country of Citizenship: **United States**	
Post Office Address:	Post Office Address: **13161 Shalimar Pl.**	City: **Del Mar**	State/Country: **California**	Postal Code: **92014**

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature of Inventor 1	Signature of Inventor 2	Signature of Inventor 3
Alexander Medvinsky	Steven E. Anderson	Paul Moroney
Date 11-26-2001	Date	Date 11-26-2001

Signature of Inventor 4	Signature of Inventor 5
Eric J. Sprunk	Jonathan A. Fellows
Date 11-29-01	Date 17 Dec 01

SF 1294046 v1

Please type a plus sign (+) inside this box → [+]

PTO/SB/81 (02-01)
Approved for use through 10/31/2002. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Client Ref. D2429

POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	09/890,180, the National Phase of PCT/US00/02174, filed January 28, 2000
Filing Date	
First Named Inventor	Alexander Medvinsky, et al.
Title	KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT SIGNALING AND CALL PACKETS BETWEEN CTA'S
Group Art Unit	
Examiner Name	
Attorney Docket Number	018926003900US

I hereby appoint:

☒ Practitioners at Customer Number 20350 → *Place Customer Number Bar Code Label here*

OR

☐ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☐ The above-mentioned Customer Number.

OR

☐ Practitioners at Customer Number →

☐ Firm *or* Individual Name					
Address					
Address					
City		State		ZIP	
Country					
Telephone		Fax			

I am the:

☐ Applicant/Inventor.

X Assignee of record of the entire interest. See 37 CFR 3.71.

Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

SIGNATURE of Applicant or Assignee of Record

Name	Charles M. Fish, Assistant Secretary
Signature	Charles M. Fish
Date	28 November, 2001

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of ____ forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any Comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

SF 1294034 v1

EXPRESS MAIL NO. EL 992 020 020